UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A Kyocera cellular device, currently in the custody of the FBI, 3600 S. Lake Drive, St. Francis, WI

Case No. 21 MJ 107

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 21, U.S.C., Section 841; Title 18, U.S.C., Section 922 and 924	

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____*)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI SA Joshua Eagen
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: April 27, 2021

Judge's signature

City and state: Milwaukee, WI

Hon. William Duffin U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, FBI Special Agent Joshua Eagen, being first duly sworn, hereby depose and state as follows:

I. BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation (FBI), and have been employed as such since March 2020. I am currently assigned to a Criminal Enterprise squad within the Milwaukee Division of the FBI and attached to the Milwaukee Area Safe Streets Task Force (MASSTF). My responsibilities include investigating violations of federal controlled substances laws and related violations, including federal firearms and money laundering offenses. I have had training regarding and participated in complex drug trafficking investigations. I have been involved with various electronic surveillance methods, the debriefing of defendants and informants, as well as others who have knowledge of the distribution, transportation, storage, and importation of controlled substances.

3. I have participated in investigations that have led to the issuance of search warrants involving violations of narcotic laws. These warrants involved the search of locations including: residences of targets, their associates and relatives, "stash houses" (houses used as drug/money storage locations), and cellular telephones. Evidence searched for and recovered in these locations has included controlled substances, drug paraphernalia, firearms, monetary instruments and various assets that were purchased with the proceeds of the drug trafficking.

4. As a Special Agent with the FBI, I am authorized to investigate violations of the laws of the United States, collect evidence in cases in which the United States is, or may be a party in interest, and execute warrants issued under the authority of the United States.

5. This affidavit is based upon my personal knowledge and upon information reported to me by other federal and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. The property to be searched (the "Subject Device") is listed below and was recovered during the arrest of federal fugitive Luis Lorenzo (2/4/1986), which took place on April 21, 2021. The device is a mostly dark-colored Kyocera brand flip-style cellular telephone with the "Verizon" service provider listed on the phone case and an unknown serial number. The Subject Device was discovered on LORENZO's person during his arrest.

II. PROBABLE CAUSE

8. Lorenzo is a felon, having been convicted of, *inter alia*, manufacture/deliver of cocaine (Milwaukee County Circuit Court Case No. 2005CF005628) and felony bail jumping (same). Lorenzo also had a warrant issued for his arrest, pursuant to a pending heroin distribution

charge in *United States v. Locke, et al.,* 20-cr-41, Dkt. 1 at *21 (E.D. Wis.).

9. Law enforcement was surveilling street address 4210 South Ravinia Drive, Unit 105, Greenfield, Wisconsin (the "Residence") the morning of April 21, 2021 after developing intelligence that Lorenzo might be present there. And in fact, law enforcement saw Lorenzo exit the Subject Residence that morning, wearing a black fanny pack. Lorenzo entered a blue Nissan Rouge with Michigan registration EBV 0861 (the "Vehicle"), which was parked outside the Residence.

10. Law enforcement approached the Vehicle and arrested Lorenzo, pursuant to the outstanding warrant. In a search of Lorenzo's person incident to his arrest, law enforcement recovered the Subject Device and approximately $2,000 cash, in small denominations. In my training and experience, when an individual with a prior drug trafficking conviction simultaneously possesses (i) this amount of cash, in small denominations, and (ii) a fanny pack that allows the individual to transport unknown items surreptitiously, that same individual is likely engaging in activities related to drug trafficking.

11. After Lorenzo's arrest, law enforcement decided to have the Vehicle towed. They then searched the Vehicle and the previously mentioned black fanny pack, which was located inside the Vehicle, pursuant to the "inventory search exception." Inside the black fanny pack were: (i) three baggies, which contained a white chalky substance law enforcement believes to be crack cocaine, weighing approximately 17 grams, 3 grams, and 13 grams, respectively; (ii) an indeterminate amount of a leafy green substance believed to be marijuana; and (iii) a digital scale. Per my training and experience, I believe this volume of drugs and the presence of a digital scale are both reflective of an intent to distribute those same drugs.

12. Given the public nature of Lorenzo's arrest, and the fact that Lorenzo had just exited

the Residence with a distribution amount of suspected controlled substances, law enforcement entered the Residence and secured the scene, to prevent the destruction of evidence.

13. Upon entry, law enforcement observed, in plain view on the counter of the Residence, a Smith & Wesson pistol and loose "powder" believed to be a controlled substance. Law enforcement also observed, in plain view, additional material indicative of drug trafficking, including pyrex dishes; packaging materials consistent with drug trafficking; and another digital scale.

14. Also inside the residence was a man named Juan Diego Santos. Santos told law enforcement that (i) he had cocaine on his person; and (ii) the gun on the counter was his. Law enforcement searched Santos' person and recovered a small amount of what appeared to be cocaine.

15. In my training and experience, very few firearms are manufactured in the state of Wisconsin, and Smith & Wesson's, in particular, are not of this limited subset.

16. In my training and experience, I know that persons engaged in illegal activities, including the possession of controlled substances and the possession of prohibited weapons, will frequently utilize their cellular telephones to perpetuate and conceal such crimes. I further suspect that Lorenzo has specifically used a personal cellular telephone to discuss his current drug trafficking, as I know, from conversations with other agents, that Lorenzo used a cellular telephone in connection with his prior drug trafficking at issue in Case No. 20-cr-41.

17. The Subject Device is currently in storage at the Milwaukee Division of the FBI. In my training and experience, I know that the device has been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of the FBI.

18. Based on my training and experience, I believe that the Subject Device is likely to contain evidence of drug trafficking, as I know that: (1) drug traffickers frequently use cellular telephones to facilitate their illicit activities; (2) the volume of controlled substances discovered in Lorenzo's possession at the time of his arrest was consistent with the distribution of the same; and (3) the indicia of drug trafficking observed in plain view at the apartment from which Lorenzo was seen exiting prior to his arrest was consistent with such illicit activities.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Digital camera*: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time,

combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. *Tablet*: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "Wi-Fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

20. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications, I know that the Subject Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, tablet and PDA. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. There is probable cause to believe that things that were once stored on the Subject Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage mediums can provide evidence of a file that was once on the storage mediums but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual

memory paging systems can leave traces of information on the storage mediums that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Subject Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Subject Device to human inspection in order to determine whether it is evidence described by the warrant. Because the instant application concerns material already in law enforcement's possession, I submit that cause exists to permit the requested search at any time of the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Subject Device described in paragraph 7 and Attachment A.

ATTACHMENT A

The Subject Device which is currently stored in evidence, under inventory number 1B270, at the Milwaukee Division of the FBI located at 3600 South Lake Drive, St. Francis, Wisconsin 53235: a mostly dark-colored Kyocera brand flip-style cellular telephone with “Verizon” service provider listed on the phone case and an unknown serial number.

ATTACHMENT B

All records on the Subject Device described in Attachment A that relate to violations of Title 21, United States Code, Section 841(a)(1) and (b)(1)(C), Title 18, United States Code, Section 924(c)(1)(A)(i), and Title 18, United States Code, Sections 922(g)(1) and 924(a)(2), to include:

a. Electronic drug or money ledgers, drug distribution or customer lists and related identifying information, drug supplier lists (including names, addresses, phone numbers, or any other identifying information); correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

b. Electronic telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, e-mails, documents, and other items or lists reflecting names, addresses, telephone numbers, addresses, and any communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

c. Records, items and documents stored on the Subject Devices reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel from August 2020 to the present;

d. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, UPS, FedEx, and other mail service receipts and records, bank statements, checks, credit card records, safe deposit box records, records and receipts and rental agreements for storage facilities, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances.

e. Photographs, videotapes or other depictions of assets, co-conspirators, controlled substances, or other activities related to drug trafficking or firearms offenses.

f. Records of Internet Protocol addresses used; records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user typed web addresses.

g. Records and Information reflecting evidence of user attribution, showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.